UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF NEW YORK

LATUSHA VAINS, On Behalf of Herself and All Others Similarly Situated,

Plaintiff,

v.

HUDSONS'S BAY COMPANY, a Canadian corporation, and SAKS FIFTH AVENUE, LLC, a Massachusetts limited liability company,

Defendants.

Case No.: 18-cv-3366

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Plaintiff, Latusha Vains ("Plaintiff"), on behalf of herself and all others similarly situated, files this Class Action Complaint against Defendants, Hudson's Bay Company ("HBC"), and Saks Fifth Avenue, LLC ("Saks") (collectively "Defendants"), and based upon personal knowledge with respect to herself and on information and belief derived therefrom, among other things, investigation of counsel and review of public documents as to all other matters, alleges as follows:

SUMMARY OF THE CASE

1. Plaintiff brings this class action case against Defendants for their failures to secure and safeguard customers' payment card data ("PCD") and other personally identifiable information ("PII") that Defendants collected at the time Plaintiff made purchases at Saks stores, and for failing to provide timely, accurate, and adequate notice to Plaintiff and the Class members that their PCD and PII (hereinafter, collectively, "Customer Data") had been compromised and stolen.

2. HBC is a retail group company and the parent of fashion retailers such as Saks Fifth Avenue and Lord & Taylor department stores, and Saks OFF 5TH outlet stores.

3. Saks is a luxury retailer, renowned for selling American and European designer clothing for men and women throughout its stores in 22 states.

4. HBC acquired Saks in 2013 for $2.4 billion dollars.

5. In the last few years, retailers such as Target, Home Depot, Kmart, Neiman Marcus, and Brooks Brothers have experienced streams of attacks on their data security. Implementing measures to prevent those attacks, as well as quickly identifying them, is a normal, expected part of the business—except in Defendants' case. Inexplicably turning a blind eye to this key aspect of their business, Defendants did not just ignore security weaknesses, they failed to setup the systems necessary to even detect them.

6. On April 1, 2018, Defendants acknowledged that approximately 5 million customers who used payment cards for transactions at Saks (and other HBC) stores throughout the United States had their Customer Data stolen (the "Data Breach"). Defendants only acknowledged the Data Breach, however, after a well-known hacking syndicate, known as Fin7 or Joker's Stash, announced the Data Breach on March 28, 2018, and a research firm, Gemini Advisory, confirmed the Data Breach on

March 31, 2018.[1]

7. This private Customer Data was compromised due to Defendants' acts and omissions and their failure to properly protect the Customer Data.

8. Defendants could have prevented this Data Breach. Data breaches at other retail establishments in the last few years have been the result of infiltration of Point-of-Sale ("POS") systems at which payment cards are swiped. While many retailers, restaurant chains and other companies using POS systems have responded to recent breaches by adopting technology that helps make transactions more secure, Defendants did not.

9. In addition to Defendants' failures to prevent the Data Breach, Defendants also failed to detect the Data Breach for at least a year, and only learned of it after security firm Gemini Advisory announced that it had found Customer Data for sale on a dark web marketplace operated by a hacking group called Joker's Stash.

10. The Data Breach was the inevitable result of Defendants' inadequate approach to data security and the protection of the Customer Data that it collected during the course of their business. The deficiencies in Defendants' data security were so significant that the malware installed by the hackers remained undetected and intact for months.

11. The susceptibility of POS systems to a breach is well-known throughout the retail industry. In the last five years, practically every major data breach involving retail stores or fast-food restaurant chains has been the result of malware placed on POS systems. Accordingly, data security experts have warned companies, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[2] Unfortunately, Defendants' profit-driven decisions to ignore these warning led to the damage upon which this case is based.

[1] Vindu Goel and Rachel Abrams, *Card Data Stolen from 5 Million Saks and Lord & Taylor Customers*, THE NEW YORK TIMES, https://www.nytimes.com/2018/04/01/technology/saks-lord-taylor-credit-cards.html (last visited April 13, 2018).
[2] Datacap Systems Inc., *Point of sale security: Retail data breaches at a glance*, https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance# (last visited April 13, 2018).

12. Saks has recognized that it is committed to "respecting and protecting the privacy of [customer's] personal information."[3] Through their Privacy Policy, Saks also represents that it will "protect the security or integrity of the [website] and [its] business, such as by protecting against and preventing fraud, unauthorized transactions, claims and other liabilities, and managing risk exposure, including by identifying potential hackers and other unauthorized users."[4]

13. Unfortunately, Saks, as well as its parent HBC, did not hold true to these promises.

14. Instead, Defendants disregarded the rights of Plaintiff and the Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure Defendants' data systems were protected, failing to disclose to their customers the material fact that they did not have adequate computer systems and security practices to safeguard Customer Data, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

15. In addition, Saks exacerbated the injuries Plaintiff and the Class members suffered by failing to timely detect the infiltration and failing to timely notify customers their information had been compromised. If Saks had detected the malware earlier and promptly notified the public of the Data Breach, the resulting losses would have been less significant.

16. As a result of Saks' Data Breach, the Customer Data of Plaintiff and the Class members has been exposed to criminals for misuse. The injuries Plaintiff and the Class members suffered as a direct result of the Saks Data Breach include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their debit or credit card accounts because

[3] Saks Fifth Avenue Privacy Policy, *available at* https://www.saksfifthavenue.com/Policies (last visited April 13, 2018).
[4] *Id.*

their account were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Saks Data Breach;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Saks Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiff's and the Class members' information on the Internet black market;

h. money paid for merchandise purchased at Saks stores during the period of the Data Breach, in that Plaintiff and the Class members would not have shopped at Saks had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Customer Data, or Plaintiff and the Class members would have taken measures to protect their Customer Data had Defendant made such disclosures;

i. damages to and diminution in value of their Customer Data entrusted to Saks for the sole purpose of purchasing merchandise from Saks; and

j. the loss of Plaintiff's and the Class members' privacy.

17. The injuries to Plaintiff and the Class members were directly and proximately caused by Saks' failure to implement or maintain adequate data security measures for Customer Data.

18. Further, Plaintiff retains a significant interest in ensuring that her Customer Data, which, while stolen, remains in the possession of Defendant, is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and other similarly situated consumers whose Customer Data was stolen as a result of the Saks Data Breach.

19. Plaintiff, on behalf of herself and other similarly situated consumers, seeks to recover damages, equitable relief including injunctive relief to prevent a reoccurrence of the Data Breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants.

21. This Court has personal jurisdiction over Saks because Saks: 1) is headquartered in this District; 2) conducts substantial business in this District; and 3) committed the acts and omissions complained of in this District.

22. This Court has personal jurisdiction over HBC because HBC: 1) maintains its United States headquarters in this District; 2) conducts substantial business in the District; and 3) committed the acts and omissions complained of in the District.

23. Venue is proper under 28 U.S.C. § 1391(c) because Defendants' principal places of business is in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions Defendants' management and IT personnel made that led to the Data Breach.

PARTIES

A. Plaintiff

24. Plaintiff Latusha Vains is a resident of the state of California.

B. Defendant

25. HBC is a Canadian corporation, which owns and operates department stores across the United States. HBC maintains its United States headquarters at 225 Liberty Street, New York, NY 10281, which is located in this District.

26. Saks is a Massachusetts limited liability company registered with the New York Department of State's Division of Corporations, State Records and Uniform Commercial Code, to do business in this state. Saks' principal place of business and headquarters is also located at 225 Liberty Street, New York, NY 10281, which is located in this District.

FACTUAL BACKGROUND

A. Plaintiff's Transactions

27. During the Christmas shopping season, Plaintiff made a purchase at Saks' store located in San Francisco, California. For this purchase, she used her American Express credit card.

28. In January 2018, Plaintiff reviewed her American Express statement and identified fraudulent activity in the amount of $1,300. Due to this fraudulent activity, Plaintiff canceled her American Express card, requested a new one, and changed her passwords associated with her American Express card and account.

29. The compromise of Plaintiff's payment card occurred even though she had physical possession of the card at all times. Plaintiff was required to expend time communicating with the card issuer attempting to resolve the issues caused by the theft of her credit card and other personal information used to accomplish the fraudulent activity.

30. Plaintiff would not have used her payment card to make purchases at Saks had Defendants told her they lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft. Indeed, Plaintiff would not have shopped at Saks at all during

the period of the Data Breach and, thus, she suffered actual injury and damages in paying money to for the purchase of merchandise from Saks that she would not have paid had Defendants made such disclosure.

31. Plaintiff suffered actual injury from having her Customer Data compromised and stolen in and as a result of the Data Breach.

32. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her Customer Data—a form of intangible property that Plaintiff entrusted to Defendants as a form of payment for merchandise and that was compromised in and as a result of the Data Breach.

33. Plaintiff further suffered actual injury in the form of time spent dealing with fraud resulting from the Data Breach, disputing the fraudulent charges on her American Express account, and monitoring her account for additional fraud.

34. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Customer Data being placed in the hands of criminals who have already misused such information, as evidenced by the compromise of Plaintiff's payment cards.

35. Moreover, Plaintiff has a continuing interest in ensuring that her private information, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

B. Defendants Collect and Store PII for their Own Financial Gain

36. Founded in 1924, Saks now operates 41[5] stores in 22 states in the United States.[6]

37. On November 4, 2013, HBC—North America's longest continually operated company—acquired Saks. HBC's acquisition of Saks added to HBC's already "iconic portfolio," which included, *inter alia*, retailer Lord & Taylor.[7]

38. On December 3, 2014, HBC, through its subsidiaries and affiliates, closed on a $1.25

[5] HBC Investor Relations, http://investor.hbc.com/releasedetail.cfm?ReleaseID=1062154 (last visited April 13, 2018).
[6] About Us, History of Saks Fifth Avenue, https://www.saksfifthavenue.com/include/aem/aem_static.jsp?page=about-us (last visited April 13, 2018);
[7] *Id.*

billion dollar, 20-year mortgage loan secured on the fee interest property of Saks' flagship store located at 611 Fifth Avenue, New York, NY 10022, demonstrating the substantial real estate holdings and overall worth of Saks and, through the acquisition, HBC.[8]

39. Since HBC's acquisition of Saks, and over the last five fiscal quarters, Saks has continually improved comparable sales and profitability. In fact, HBC recently reported retail sales of $4.695 billion Canadian dollars—or approximately $3.779 billion U.S. dollars.[9]

40. Despite Saks' and HBC's continuing improvements and profitability, Defendants failed to make meaningful improvements to the security of Defendants' POS systems and administrative network, placing the purchasing information of their customers at risk. Instead, HBC announced a cost-cutting "Transformation Plan" for its North American operations with the expectation of reducing 2,000 positions and generating more than $350 million in annual savings.[10]

41. A significant portion of sales at Defendants' brick-and-mortar stores, as well as their online stores, are made using credit or debit cards. When customers pay using credit or debit cards, Defendants collect Customer Data related to those cards including the cardholder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards. Defendants then store the Customer Data in their POS system and transmit that information to a third party for processing and completion of the payment.

42. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Customer Data collected, maintained, and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

---

[8] HBC, *Positioning HBC for the Future*, http://files.shareholder.com/downloads/AMDA-1ETYKL/6193711304x0x942709/4EEC9E08-15BE-4D94-9921-F9D90504D6C5/HBC.2016AR.Full.pdf (last visited April 13, 2018).

[9] HBC Reports Fourth Quarter and Fiscal 2017 Financial Results, *available at:* http://investor.hbc.com/releasedetail.cfm?releaseid=1062154 (March 28, 2018) (last visited April 13, 2018)

[10] HBC Announces Transformation Plan for North American Operations to Deliver Best-in-Class All-Channel Customer Service, *available at*: https://www.businesswire.com/news/home/20170608006311/en/HBC-Announces-Transformation-Plan-North-American-Operations (last visited April 13, 2018).

43. It is well known and the subject of many media reports that Customer Data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches by other retailers, Defendants maintained an insufficient and inadequate system to protect Plaintiff's and the Class members' Customer Data.

44. Customer Data is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, and other personal information on a number of underground Internet websites. Customer Data is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

45. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[11]

46. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on their customers as a result of a data breach.

47. Defendants were, or reasonably should have been, fully aware of the significant volume of daily credit and debit card transactions at Saks' retail locations and, thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

48. Unfortunately, and as alleged below, despite all of this publicly available knowledge of

[11] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 13, 2018).

the continued compromises of Customer Data in the hands of other third parties, such as retailers, Saks' approach to maintaining the privacy and security Plaintiff's and the Class members' Customer Data was lackadaisical, cavalier, reckless, or at the very least, negligent.

C. Defendants Had Notice of Data Breaches Involving Malware on POS Systems

49. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[12] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[13] The amount of payment card data compromised by data breaches is massive. For example, it is estimated that over 100 million cards were compromised in 2013 and 2014.[14]

50. Most of the massive data breaches occurring within the last several years involved malware placed on POS systems used by retail merchants. A POS system is an on-site device, much like an electronic cash register, which manages transactions from consumer purchases, both by cash and card. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor." [15] The payment processor then passes on the payment information to the financial institution that issued the card and takes the other steps needed to complete the transaction.[16]

51. Before transmitting customer data over the merchant's network, POS systems typically, and very briefly, store the data in plain text within the system's memory.[17] The stored information includes "Track 1" and "Track 2" data from the magnetic strip on the payment card, such as the

---

[12] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, Identity Theft Resource Center (Jan. 19, 2017), http://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208 (last visited April 13, 2018).
[13] *Id*.
[14] Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20, 2014), available at: https://origin-www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf (last visited April 13, 2018).
[15] *Id*. at 6.
[16] Salva Gomzin, *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions*, 8 (Wiley 2014), *available at:* http://1.droppdf.com/files/IS0md/wiley-hacking-point-of-sale-payment-application-secrets-threats-and-solutions-2014.pdf (last visited April 13, 2018).
[17] *Id*. at 39.

cardholder's first and last name, the expiration date of the card, and the CVV (three number security code on the card).[18] This information is unencrypted on the card and, at least briefly, will be unencrypted in the POS terminal's temporary memory as it processes the data. [19]

52. In order to directly access a POS device, hackers generally follow four steps: infiltration, propagation, exfiltration and aggregation.[20] In the infiltration phase, an "attacker gains access to the target environment"[21] allowing the hackers to move through a business' computer network, find an entry point into the area that handles consumer payments, and directly access the physical POS machines at in-store locations.[22] Once inside the system the attacker then infects the POS systems with malware, which "collects the desired information . . . and then exfiltrates the data to another system" called the "aggregation point."[23]

53. A 2016 report by Verizon confirmed "[t]he vast majority of successful breaches leverage legitimate credentials to gain access to the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to capture payment card data."[24] According to Verizon, hackers successfully compromise POS systems in a matter of minutes or hours and exfiltrate data within days of placing malware on the POS devices.[25]

54. Intruders with access to unencrypted Track 1 and Track 2 payment card data can physically replicate the card or use it online. Unsurprisingly, theft of payment card information via POS systems is now "one of the biggest sources of stolen payment cards."[26] Since 2014, malware installed on POS systems has been responsible for nearly every major data breach of a retail outlet or

---

[18] *Id*. at 43-50.
[19] Symantec, *supra* note 8, at 5.
[20] *Point of Sale Systems and Security: Executive Summary*, SANS Institute, 4 (Oct. 2014), available at: https://www.sans.org/reading-room/whitepapers/analyst/point-salesystems-security-executive-summary-35622 (last visited April 13, 2018).
[21] *Id*.
[22] Symantec, *supra* note 8, at 6.
[23] *Id*.
[24] *Id*.
[25] *2016 Data Breach Investigations Report*, Verizon, at 4 (Apr. 2016), http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Retail-DataSecurity_en_xg.pdf. (last visited April 13, 2018).
[26] Symantec, *supra* note 8, at 3.

restaurant.[27] In 2015, intrusions into POS systems accounted for 64% of all breaches where intruders successfully stole data.[28] For example, in 2013, hackers infiltrated Target, Inc.'s POS system, stealing information from an estimated 40 million payment cards in the United States.[29] In 2014, over 7,500 self-checkout POS terminals at Home Depots throughout the United States were hacked, compromising roughly 56 million debit and credit cards.[30]

55. Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, Defendants were well aware or should have been aware of the need to safeguard their POS systems.

D. Defendants Failed to Comply with Industry Standards

56. Despite the vulnerabilities of POS systems, available security measures and reasonable businesses practices would have significantly reduced or eliminated the likelihood that hackers could successfully infiltrate business' POS systems. One report indicated that over 90% of the data breaches occurring in 2014 were preventable.[31]

57. The payment card networks (MasterCard, Visa, Discover, and American Express), data security organizations, state governments, and federal agencies have all implemented various standards and guidance on security measures designed to prevent these types of intrusions into POS systems. However, despite Defendants' understanding of the risk of data theft via malware installed on POS systems, the widely available resources to prevent intrusion into POS data systems, and the multiple breaches of the POS systems at other retailers, Defendants failed to adhere to these guidelines and failed to take reasonable and sufficient protective measures to prevent the Data Breach.

---

[27] Verizon, *supra* note 19, at 1.
[28] *Id*. at 3.
[29] Brian Krebs, *Fast Food Chain Arby's Acknowledges Breach*, KrebsOnSecurity (Feb. 17, 2017), https://krebsonsecurity.com/2017/02/fast-food-chain-arbysacknowledges-breach/ (last visited April 13, 2018).
[30] Brett Hawkins, *Case Study: The Home Depot Data Breach,* 7 (SANS Institute, Jan. 2015), available at: https://www.sans.org/reading-room/whitepapers/casestudies/casestudy-home-depot-data-breach-36367 (last visited April 13, 2018).
[31] Verizon, *supra* note 5, at 1.

58. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, more than two years ago, Symantec recommended "point to point encryption" implemented through secure card readers, which encrypts credit card information in the POS system, preventing malware that extracts card information through the POS memory while it processes the transaction.[32] Moreover, Symantec emphasized the importance of adopting EMV chip technology. Likewise, Datacap Systems, a developer of POS systems, recommended similar preventative measures.[33]

59. The major payment card industry brands set forth specific security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: 1) protect cardholder data and prevent its unauthorized disclosure; 2) store data, even in encrypted form, no longer than necessary to process the transaction; and 3) comply with all industry standards.

60. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.[34]

61. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[35] PCI DSS sets the minimum level of what must be done, not the maximum.

[32] Symantec, *supra* note 8, at 6.
[33] *See* Datacap Systems, *supra* note 2.
[34] *Payment Card Industry Data Security Standard* v3.2, at 5 (April 2016) available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited April 13, 2018).
[35] *Id*.

62. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, impose the following mandates on Defendants: [36]

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

63. Among other things, PCI DSS required Defendants to properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

64. PCI DSS also required Defendants not to store "the full contents of…the magnetic stripe located on the back of a card" or "the card verification code or value" after authorization.[37]

65. Despite Defendants' awareness of their data security obligations, Defendants' treatment of PCD and PII entrusted to them by their customers fell far short of satisfying Defendants' legal duties and obligations, and included violations of the PCI DSS. Defendants failed to ensure that access to their data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings, and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

[36] *Id*.
[37] *Id*. at 38 (PCI DSS 3.2.1 and 3.2.2).

E. HBC Failed to Patch Data Security Holes When Implementing EMV Technology

66. The payment card industry also set rules requiring all businesses to upgrade to new card readers that accept EMV chips. Data Security advisors, like Symantec and DataCap Systems, have strongly encouraged the use of POS terminals capable of accepting payment from EMV chips.

67. EMV chip technology uses embedded computer chips instead of magnetic stripes to store PCD. The magnetic stripe on the back of a debit or credit card contains a code that is recovered by sliding the card through a magnetic stripe reader. The code never changes. Unlike magnetic stripe technology, in which the card information never changes, EMV technology creates a unique transaction code every time the chip is used. Such technology increases payment card security because the unique transaction code cannot be used again, making it more difficult for criminals to use stolen EMV chip card information.

68. The EMV standard was mandated by credit card processors and banks to be implemented in the United States in 2015.

69. It has been reported that all the Saks locations were using the EMV; however, this technology alone does not make Customer Data secure.

70. EMV technology, as standardly implemented, is missing a really important piece: the requirement to encrypt data from the point of sale to the credit card processor switch. That means, if a retailer's network has been infiltrated, without encryption, credit card numbers can still be read and stolen.

71. With knowledge of this vulnerability in EMV technology, most large retailers have taken the initiative to implement an encryption standard known as Point-to-Point (or P2P) encryption with the implementation of EMV. P2P encryption converts PII and PCD data into indecipherable code at the time the card is swiped. With this encryption, even if the system is hacked and the data is compromised, the data is indecipherable, thus making it unusable by and worthless to hackers.

72. Given the Data Breach, apparently HBC had implemented EMV technology at Saks locations but had decided against implementing P2P encryption to fill the hole in Defendants' data security.

73. As Greg Buzek, president of IHL Services, pointed out: "We have always recommended P2P encryption *and* tokenization, regardless of whether a retailer chose to be EMV compliant. That was the only thing that brought security. Having EMV without encryption and tokenization was simply fool's security. And if Saks indeed was EMV compliant and did not have P2P encryption and tokenization, this is indeed a perfect example of that."[38]

F. Defendants Failed to Comply With FTC Requirements

74. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[39]

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[40] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is

[38] Confusion Reigns In The Wake Of Saks, Lord and Taylor Data Breach, Forbes, (April 2, 2018), *available at*: https://www.forbes.com/sites/paularosenblum/2018/04/02/confusion-reigns-in-the-wake-of-saks-lord-and-taylor-data-breach/#2434859b337a (last visited April 10, 2018).
[39] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 13, 2018).
[40] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 13, 2018).

attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

76. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[41]

77. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

78. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential Costumer Data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

79. In this case, Defendants were at all times fully aware of their obligations to protect the financial data of Saks' customers because of their participation in payment card processing networks. Defendants were also aware of the significant repercussions if they failed to do so because Defendants collected payment card data from tens of thousands of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and the Class members.

80. Despite understanding the consequences of inadequate data security, Defendants failed to comply with PCI DSS requirements and failed to take additional protective measures beyond those required by PCI DSS.

[41] FTC, *Start With Security*, *supra* note 34.

81. Despite understanding the consequences of inadequate data security, Defendants operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and failed to take other measures necessary to protect their data network.

G. Defendants' Data Breach

82. On March 28, 2018, the criminal syndicate Joker's Stash announced that five million stolen credit and debit cards would be released for sale on the dark web.

83. Joker's Stash is one of the largest criminal syndicates in the hacking world, and has carried out attacks against Omni Hotels and Resorts, Chipotle, Whole Foods, and others.[42] The group consists of software developers, money launderers, operational security personnel and executives, and every law enforcement agency is seeking to find their members and cease their operations.[43]

84. Despite these agencies seeking Joker's Stash, Joker's Stash focuses on loyalty programs, frequent-buyer discounts, money-back guarantees, and customer service to actively court bulk buyers and organized crime rings.[44] Joker's Stash then sells the hacked Customer Data, which is then used to create counterfeit cards and fraudulently purchase gift cards, electronics, and other goods at big-box retailers like Target and Wal-Mart; Joker's Stash boasts that their cards are "exclusive, self-hacked dumps," exclusive to Joker's Stash end customers.[45]

85. The security firm Gemini Advisory suggested the Joker's Stash criminal syndicate has been siphoning Customer Data from Defendants since as early as May 2017.[46]

86. This Data Breach is not the first time Saks has been involved in a data security incident. In March of 2017, Saks announced that online shoppers had her personal information made publicly available online and compromised as a result of unencrypted connections on its online website, which

---

[42] Tim Stelloh, *Data Breach at Saks, Lord & Taylor Compromises Customer Payment Data*, https://www.nbcnews.com/news/us-news/data-breach-saks-lord-taylor-compromises-customer-payment-data-n861856 (last visited April 13, 2018).
[43] *Id.*
[44] Brian Krebs, *Carders Park Piles of Cash at Joker's Stash*, https://krebsonsecurity.com/2016/03/carders-park-piles-of-cash-at-jokers-stash/ (last visited April 13, 2018)
[45] *Id.*
[46] Gemini Advisory, *Fin7 Syndicate Hacks Saks Fifth Avenue and Lord & Taylor Stores*, https://geminiadvisory.io/fin7-syndicate-hacks-saks-fifth-avenue-and-lord-taylor/ (last visited April 13, 2018)

HBC maintains. These security vulnerabilities exposed customers' email addresses, phone numbers, IP addresses of the computers used for online shopping, as well as the product codes for items the customers browsed while shopping.

87. Additionally, just months before the announcement of the Data Breach, BuzzFeed News broke news that Saks had been storing customer data in plain text on servers, which highlighted Saks' lackadaisical approach to protecting the data of its millions of customers.[47]

H. The Data Breach Caused Harm and Will Result in Additional Fraud

88. Without detailed disclosure of the nature and scope of the Data Breach, consumers, including Plaintiff and the Class members, have been left exposed—unknowingly and unwittingly—for months to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

89. The ramifications of Defendants' failure to keep Plaintiff's and the Class members' Costumer Data secure are severe.

90. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[48] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[49]

91. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[50]

---

[47] Jon Fingas, *Saks Fifth Avenue left Customer Data Exposed to the Public*, https://www.engadget.com/2017/03/19/saks-fifth-avenue-left-customer-data-exposed (last visited April 13, 2018).
[48] 17 C.F.R § 248.201 (2013).
[49] *Id.*
[50] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 13, 2018).

92. Identity thieves can use personal information, such as Plaintiff's and the Class members', which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

93. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[51]

94. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[52]

95. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[53]

[51] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 13, 2018).
[52] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 13, 2018).
[53] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 13, 2018).

96. Plaintiff and the Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class members are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

I. Plaintiff and the Class Members Suffered Damages

97. Plaintiff and the Class members Customer Data is private and sensitive in nature, and Defendants left that Customer Data inadequately protected. Defendants did not obtain Plaintiff's and the Class members' consent to disclose their Customer Data to any other person as required by applicable law and industry standards.

98. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and the Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

99. Defendants had the resources to prevent a breach, especially with HBC's acquisition of Saks in 2013 and the influx of capital from the $1.25 billion dollar loan and other financial synergies accomplished with the acquisition. Instead, HBC lauded the downsizing of personnel and neglected to adequately invest in data security, despite the growing number of POS intrusions and several years of well-publicized data breaches.

100. Had Defendants remedied the deficiencies in their POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Defendants would have prevented intrusion into their POS systems and, ultimately, the theft of their customers' Customer Data.

101. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting Data Breach, Plaintiff and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

102. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class members' Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiff's and the Class members' information on the Internet black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their Customer Data;

f. loss of privacy;

g. the monetary amount of purchases at Saks during the period of the Data Breach in that Plaintiff and the Class members would not have shopped at Saks, or at least would not have used their payment cards for purchases, had Defendants disclosed that Saks lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Defendants provided timely and accurate notice of the Data Breach;

h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

i. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

k. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

l. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

103. Defendants have stated that affected customers will be offered credit monitoring or identity theft protection services, but have not come forth with any details as to how to sign up, the type of coverage, the scope of coverage, or the length of coverage. As a result, Plaintiff and the Class

members are left to their own actions to protect themselves from the financial damage Defendants have allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Defendants' actions have created for Plaintiff and the Class members is ascertainable and is a determination appropriate for the trier of fact. Defendants also have not offered to cover any of the damages sustained by Plaintiff or the Class members but rather have stated only that fraudulent charges *should* be covered by affected customers' financial institutions.

104. While Plaintiff's and the Class members' Customer Data has been stolen, Defendants continue to hold Customer Data of consumers, including Plaintiff and the Class members. Particularly because Defendants have demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and the Class members have an undeniable interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CHOICE OF LAW

105. New York, which seeks to protect the rights and interests of New York and other U.S. residents against a company doing business in New York, has a greater interest in the claims of Plaintiff and the Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

106. The principal place of business of both Defendants, located at 225 Liberty Street, New York, NY 10281, is the "nerve center" of Defendants' business activities—the place where high-level officers direct, control, and coordinate Defendants' activities, including data security, and where: a) major policy; b) advertising; c) distribution; d) accounts receivable departments; and e) financial and legal decisions originate.

107. Data security assessments and other IT duties related to POS systems and data security occur at Defendants' New York headquarters.

108. Furthermore, Defendants' response, and corporate decisions surrounding such response, to the Data Breach were made from and in New York.

109. Defendants' breach of their duty to customers—including Plaintiff and the Class members—emanated from New York.

110. Moreover, because Defendants are headquartered in New York and their key decisions and operations emanate from New York, New York law can and should apply to claims relating to the Data Breach, even those made by persons who reside outside of New York. In fact, New York law should apply to all of Plaintiff's claims, as Defendants' decisions and substandard acts happened in New York, and, upon information and belief, the Plaintiff's PII was collected, stored on, and routed through New York-, and United States-based servers. For the sake of fairness and efficiency, New York law should apply to these claims.

111. Application of New York law to a nationwide Class with respect to Plaintiff's and the Class members' claims is neither arbitrary nor fundamentally unfair because New York has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiff and the nationwide Class.

112. Further, under New York's choice of law principles, which are applicable to this action, the common law of New York will apply to the common law claims of all Class members.

CLASS ACTION ALLEGATIONS

113. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiff brings this lawsuit on behalf of herself and as a class action on behalf of the following Class:

> All persons residing in the United States who made a credit or debit card purchase at any affected Saks location from May 1, 2017, through April 1, 2018 (the "Nationwide Class").

114. Excluded from the Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest; Defendants' officers, agents, and employees; and all persons who make a timely election to be excluded from the Class. Also excluded from the Class are the judge assigned to this action, and any member of the judge's immediate family.

115. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. Plaintiff reasonably believes that the Class members number in

the hundreds of thousands and up to five (5) million people or more in the aggregate, and well over 1,000 in the smallest of the classes. The names and addresses of the Class members are identifiable through documents Defendants maintain.

116. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

a. Whether Defendants owed a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendants knew or should have known of the susceptibility of their POS systems to a data breach;

d. Whether Defendants' security measures to protect their POS systems were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and other measures data security experts recommended;

e. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class members' Customer Data;

f. Whether the Class members' PII was accessed, compromised, or stolen in the Data Breach;

g. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

h. Whether defendants' failure to implement adequate data security measures allowed the breach of their POS data systems to occur;

i. Whether Defendants' conduct constituted deceptive trade practices under New York law;

j. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of Plaintiff's and the Class members' Customer Data;

k. Whether Defendants failed to timely notify the public of the Data Breach;

l. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;

m. Whether Plaintiff and the Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

n. Whether Plaintiff and the Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

117. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

118. **Typicality:** Plaintiff's claims are typical of the Class members' claims because, among other things, Plaintiff and the Class members were injured through Defendants' substantially uniform misconduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and the Class members, and there are no defenses that are unique to Plaintiff's claims. Plaintiff's and the Class members' claims arise from the same operative facts and are based on the same legal theories.

119. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation; and Plaintiff will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

120. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for the Class members to individually seek redress for Defendants' wrongful conduct. Even if the Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

121. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

122. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether the Class members' PII was accessed, compromised, or stolen in the Data Breach;

b. Whether (and when) Defendants knew about the Data Breach before it was announced to the public and whether Defendants failed to timely notify the public of the Data Breach;

c. Whether Defendants misrepresented the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiff's and the Class members' Customer Data;

d. Whether Defendants concealed crucial information about their inadequate data security measures from Plaintiff and the Class members;

e. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

g. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and the Class members' Customer Data secure and prevent the loss or misuse of that information;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiff's and the Class members' Customer Data in violation of N.Y. Gen. Bus. Law § 349, and Section 5 of the FTC Act;

i. Whether Defendants failed to provide timely notice of the Data Breach, to Plaintiff and the Class members in violation of N.Y. Gen. Bus. Law § 899-aa;

j. Whether Defendants owed a duty to Plaintiff and the Class members to safeguard their Customer Data and to implement adequate data security measures;

k. Whether Defendants breached that duty;

l. Whether an implied contract existed between Defendants and Plaintiff and the Class members, and the terms of that implied contract; and,

m. Whether Defendants breached the implied contract.

CLAIMS ALLEGED ON BEHALF OF THE CLASS

First Claim for Relief
Negligence

123. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 122 as though fully stated herein.

124. Upon accepting and storing Plaintiff's and the Class members' Customer Data in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiff and the

Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Customer Data was private and confidential, and should be protected as private and confidential.

125. Defendants owed a duty of care not to subject Plaintiff and the Class members, along with their Customer Data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

126. Defendants owed a duty to Plaintiff and the Class members to exercise reasonable care in safeguarding and protecting their Customer Data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure Plaintiff's and the Class members' Customer Data was adequately secured and protected. Defendants further had a duty to implement processes that would detect a breach of their data system in a timely manner.

127. Defendants knew that Plaintiff's and the Class members' Customer Data was personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if Plaintiff's and the Class members' Customer Data was wrongfully disclosed, that disclosure was not fixed, or Plaintiff and the Class members were not told about the disclosure in a timely manner.

128. By being entrusted by Plaintiff and the Class members to safeguard their Customer Data, Defendants had a special relationship with Plaintiff and the Class members; Plaintiff and the Class members purchased Saks merchandise and accepted Saks' offer to use payment cards as an approved form of payment. Plaintiff and the Class members did so with the understanding that Defendants would take appropriate measures to protect their Customer Data and would inform Plaintiff and the Class members of any breaches or other security concerns that might call for action. But, Defendants did not. Defendants not only knew their data security was inadequate, they also knew they didn't have the tools to detect and document intrusions or exfiltration of Customer Data. Defendants are morally culpable, given their wholly inadequate safeguards, cost-cutting measures to

maximize shareholder return without regard for security, and refusal to notify Plaintiff and the Class members of breaches or security vulnerabilities.

129. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Customer Data by failing to adopt, implement, and maintain adequate security measures to safeguard that information, and allowing unauthorized access to Plaintiff's and the Class members' Customer Data.

130. Defendants also breached their duty to timely disclose that Plaintiff's and the Class members' Customer Data had been, or was reasonably believed to have been, stolen or compromised.

131. Defendants' failure to comply with industry and federal regulations further evidences Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Customer Data.

132. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the Class members, their Customer Data would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of Plaintiff's and the Class members' Customer Data, as well as the resulting damages.

133. The injury and harm Plaintiff and the Class members suffered was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Customer Data. Defendants knew their systems and technologies for processing and securing Plaintiff's and the Class members' Customer Data had numerous security vulnerabilities.

134. Defendants' misconduct as alleged herein was willful and with conscious disregard of Plaintiff's and the Class members' rights or safety, and despicable conduct that has subjected Plaintiff and the Class members to cruel and unjust hardship in conscious disregard of their rights.

135. As a result of Defendants' misconduct, Plaintiff's and the Class members' Customer Data was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Customer Data was disclosed to third parties without their consent. Plaintiff and Class

members also suffered diminution in value of their Customer Data in that it is now easily available to hackers on the dark web. Plaintiff and the Class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Second Claim for Relief
Breach of Implied Contract

136. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 122 as though fully stated herein.

137. Saks solicited and invited Plaintiff and the Class members to make purchases using their credit or debit cards. Plaintiff and the Class members accepted Saks' offers and used their credit or debit cards to make purchases at Saks stores during the period of the Data Breach.

138. When Plaintiff and the Class members purchased and paid for merchandise at Saks stores using payment cards, they provided their Customer Data, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards. In so doing, Plaintiff and the Class members entered into implied contracts with Saks pursuant to which Saks agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and the Class members if their data had been breached and compromised.

139. Each purchase Plaintiff and the Class members made at Saks using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with Saks under which Saks agreed to safeguard and protect the Customer Data of Plaintiff and the Class members, including all information contained in the magnetic stripe of Plaintiff's and the Class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

140. Plaintiff and the Class members would not have provided and entrusted their Customer Data, including all information contained in the magnetic stripes of their credit and debit cards, to Saks to make purchases in the absence of the implied contract between them and Saks.

141. Plaintiff and the Class members fully performed their obligations under the implied contracts with Saks.

142. Saks breached the implied contracts it made with Plaintiff and the Class members by failing to safeguard and protect Plaintiff's and the Class members' Customer Data by failing to provide timely and accurate notice to them that their Customer Data was compromised as a result of the Data Breach.

143. As a direct and proximate result of Saks' breaches of the implied contracts between Saks and Plaintiff and the Class members, Plaintiff and the Class members sustained actual losses and damages, including nominal damages, as described in detail above. This breach of the implied contracts was a direct and legal cause of the injuries and damages to Plaintiff and the Class members, as described above.

Third Claim for Relief
Negligence Per Se

144. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 122 as though fully stated herein.

145. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

146. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Customer Data it obtained and stored, and the foreseeable consequences of a data breach at a retail chain as large as Saks, including, specifically, the immense damages that would result to Plaintiff and the Class members.

147. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

148. Plaintiff and the Class members are within the class of persons the FTC Act was intended to protect.

149. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that Plaintiff and the Class members suffered.

150. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class members have suffered, and continue to suffer, injuries and damages arising from Plaintiff's and the Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

Fourth Claim for Relief
Unjust Enrichment

151. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 122 as though fully stated herein.

152. Plaintiff and the Class members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Saks and provided Saks with their payment information. In exchange, Plaintiff and the Class members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their Customer Data with adequate data security.

153. Defendants knew that Plaintiff and the Class members conferred a benefit on Saks and accepted and have accepted or retained that benefit. Defendants profited from the purchases and used Plaintiff's and the Class members' Customer Data for business purposes.

154. Defendants failed to secure Plaintiff's and the Class members' Customer Data and, therefore, did not provide full compensation for the benefit Plaintiff and the Class members provided.

155. Defendants acquired the Customer Data through inequitable means and failed to disclose the inadequate security practices previously alleged.

156. If Plaintiff and the Class members knew that Defendants would not secure their Customer Data using adequate security, they would not have made purchases at Saks.

157. Plaintiff and the Class members have no adequate remedy at law.

158. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and the Class members conferred.

159. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and the Class members, proceeds that Defendants unjustly received from Plaintiff and the Class members. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and the Class members overpaid.

Fifth Claim for Relief
Declaratory Judgment

160. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 122, and 136 through 143, as though fully stated herein.

161. As previously alleged, Plaintiff and the Class members entered into an implied contract that required Saks to provide adequate security for the Customer Data it collected from their payment card transactions. As previously alleged, Saks owes duties of care to Plaintiff and the Class members that require it to adequately secure Customer Data.

162. Saks still possesses Customer Data pertaining to Plaintiff and the Class members.

163. Saks has made no announcement or notification that it has remedied the vulnerabilities in Defendants' computer data systems, and, most importantly, their POS systems.

164. Accordingly, Saks has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members. In fact, now that Saks' lax approach towards data security has become public, the Customer Data in Defendants' possession is more vulnerable than previously.

165. Actual harm has arisen in the wake of the Data Breach regarding Saks' contractual obligations and duties of care to provide data security measures to Plaintiff and the Class members.

166. Plaintiff, therefore, seeks a declaration that: a) Saks' and its parent HBC's existing data security measures do not comply with Saks' contractual obligations and duties of care; and b) in order to comply with Saks' contractual obligations and duties of care, Saks and its parent HBC must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training Defendants' security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. purging, deleting, and destroying in a reasonable secure manner Customer Data not necessary for Defendants' provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating Defendants' customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants' customers must take to protect themselves.

Sixth Claim for Relief
Violation of New York's Data Breach Laws – Delayed Notification
(N.Y. Gen. Bus. Law § 899-aa)

167. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 122 as though fully stated herein.

168. Section 899-aa(3) of the New York General Business Law requires any "person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization."

169. The security breach notification shall be directly provided to the affected persons by: a) written notice; b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction; c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. N.Y. Gen. Bus. Law § 899-a(5).

170. The Data Breach described herein this Complaint constitutes a "breach of the security system" of Defendants.

171. As alleged above, Defendants unreasonably delayed informing Plaintiff and the Class members about the Data Breach, affecting the confidential and non-public Customer Data of Plaintiff and the Class members after Defendants knew the Data Breach had occurred.

172. Defendants failed to disclose to Plaintiff and the Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Customer Data when Defendants knew or reasonably believed such information had been compromised.

173. Defendants' ongoing business interests gave Defendants incentive to conceal the Data Breach from the public to ensure continued revenue.

174. Upon information and belief, no law enforcement agency instructed Defendants that notification to Plaintiff and the Class members would impede Defendants' investigation.

175. As a result of Defendants' violation of New York law, Plaintiff and the Class members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, including closing their payment card accounts, not using payment cards as payment for merchandise at Saks stores, securing identity theft protection, or requesting a credit freeze. These measures would have prevented some or all of the damages Plaintiff and the Class members suffered because their stolen information would not have any value to identity thieves.

176. As a result of Defendants' violation of New York law, Plaintiff and the Class members have suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

177. Plaintiff and the Class members seek all remedies available under New York law, including, but not limited to damages Plaintiff and the Class members suffered as alleged above, as well as equitable relief.

Seventh Claim for Relief
Violation of New York Business Law
Deceptive and Unlawful Business Practice
(N.Y. Gen. Bus. Law § 349)

178. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 122 as though fully stated herein.

179. As discussed above, Defendants' acts, practices, and omissions at issue in this matter, particularly those related to data security, were directed and emanated from Defendants' headquarters in New York, NY.

180. New York General Business Law ¶ 349 ("NYGBL ¶ 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

181. In the conduct of their business, trade, and commerce, and in the sale of goods and services to consumers emanating from their headquarters in the state of New York, Defendants collected and stored highly personal and private information, including Customer Data, belonging to Plaintiff and the Class members.

182. By using their payment cards as methods of payment, which Saks accepted, Plaintiff and the Class members entrusted Defendants with their private Customer Data.

183. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the NYGBL ¶ 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL ¶ 349.

184. Defendants stored Plaintiff's and the Class members' Customer Data in Defendants' electronic and consumer information databases. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiff's and the Class members' Customer Data secure and prevented the loss or misuse of Plaintiff's and the Class members' Customer Data. Defendants did not disclose to Plaintiff and the Class members that their data systems were not secure.

185. Plaintiff and the Class members were entitled to assume, and did assume, Defendants would take appropriate measures to keep their Customer Data safe. Defendants did not disclose at any time that Plaintiff's and the Class members' Customer Data was vulnerable to hackers because Defendants' data security measures were inadequate, and Defendants were the only ones in possession of that material information, which they had a duty to disclose.

186. Defendants violated the NYGBL ¶ 349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendants' many systems and services, specifically the security thereof, and their ability to safely store Plaintiff's and Class members' Customer Data.

187. Defendants also violated the NYGBL ¶ 349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and the Class members of the Data Breach. If Defendants had complied with these legal requirements, Plaintiff and the other Class members would not have suffered the damages related to the Data Breach.

188. Further, as alleged herein, Defendants engaged in unlawful business practices in the conduct of business transactions, in violation of the NYGBL ¶ 349, by and including, their:

a. failure to maintain adequate computer systems and data security practices to safeguard Customer Data;

b. failure to disclose that Defendants' computer systems and data security practices were inadequate to safeguard Customer Data from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiff and the Class members;

d. continued acceptance of credit and debit card payments and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the POS systems that were exploited in the Data Breach; and

e. continued acceptance of credit and debit card payments and storage of other personal information after Defendants knew or should have known of the Data Breach and before they allegedly remediated the Data Breach.

189. Furthermore, as alleged above, Defendants' failure to secure consumers' Customer Data violates the FTCA and therefore violates the NYGBL ¶ 349.

190. Defendants knew or should have known that their computer and POS systems and data security practices were inadequate to safeguard Plaintiff's and the Class members' Customer Data, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

191. Because Defendants accepted credit and debit cards as methods of payment, Plaintiff and the Class members relied upon Defendants to advise customers if their POS and data systems were not secure and, thus, Customer Data could be compromised.

192. Plaintiff and the Class members were not afforded by Defendants equal or ample opportunity to make any inspection to determine Defendants' data security or to otherwise ascertain the truthfulness of Defendants' direct and indirect representations regarding data security, including Defendants' failure to alert customers that their POS and data systems were not secure and, thus, were vulnerable to attack.

193. In deciding to use their payment cards for their purchases at Saks, Plaintiff and the Class members relied upon Defendants' direct and indirect representations regarding data security, including Defendants' failure to alert customers that their POS and data systems were not secure and, thus, were vulnerable to attack.

194. Had Defendants disclosed to Plaintiff and the Class members that their POS and data systems were not secure and, thus, vulnerable to attack, Plaintiff and the Class members would not have used their payment cards at Saks, and very well may not have made purchases at all at Saks stores.

195. As a direct result of their reliance upon Defendants to be truthful in their disclosures and non-disclosures regarding the vulnerability of their POS and data systems, Plaintiff and the Class members used their payment cards to make purchases at Saks during the Data Breach period and their Customer Data was compromised, which caused Plaintiff and the Class members to suffer damages.

196. By engaging in the conduct delineated above, Defendants have violated NYGBL ¶ 349 by, among other things:

a. Omitting material facts regarding the goods and services sold;

b. Omitting material facts regarding the financial transactions, particularly the security thereof, between Saks and its customers for the purchases of goods and services;

c. Misrepresenting material facts in the furnishing or sale of goods and services to consumers;

d. Engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

e. Engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. Unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably unavoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

g. Other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

197. As a direct and proximate result of Defendants' violation of NYGBL ¶ 349, Plaintiff and the Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of Plaintiff's and the Class members' Customer Data; damages arising from Plaintiff's inability to use her credit card because that card was cancelled, suspended, or otherwise rendered

unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

198. As a result of Defendants' unlawful business practices, violations of the NYGBL ¶ 349, Plaintiff and the Class members are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class members, respectfully requests that this Court enter an Order:

a. Certifying the Class, and Plaintiff and her Counsel to represent the Class;

b. Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

c. Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

d. Awarding Plaintiff and the Class members actual, compensatory, consequential, and/or nominal damages;

e. Awarding Plaintiff and the Class members statutory damages and penalties, as allowed by law;

f. Requiring Defendants to provide appropriate credit monitoring services to Plaintiff and the Class members;

g. Compelling Defendants to use appropriate cyber security methods and policies with respect to data collection, storage, and protection, and to disclose with specificity to the Class members the type of Customer Data compromised

h. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

i. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs and expenses, and;

j. Granting such other relief as the Court deems just and proper.

Dated: Manhasset, NY
April 17, 2018

/s Paul C. Whalen
Paul C. Whalen (PW1300)
LAW OFFICE OF PAUL C. WHALEN, P.C.
768 Plandome Road
Manhasset, NY 11030
Tel: (516) 426-6870
pcwhalen@gmail.com

JOHN A. YANCHUNIS*
jyanchunis@ForThePeople.com
RYAN MCGEE*
rmcgee@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505

JEAN SUTTON MARTIN*
jean@jsmlawoffice.com
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road Suite 225
Wilmington, NC 28403
Telephone: (910) 292-6676

Attorneys for Plaintiff and the Proposed Class
* *pro hac vice* application to be submitted